



G O B I E R N O D E L A P R O V I N C I A D E B U E N O S A I R E S
2019 - Año del centenario del nacimiento de Eva María Duarte de Perón

Resolución

Número:

Referencia: EX-2019-10925058-GDEBA-DGTYAMJGM

VISTO el EX-2019-10925058-GDEBA-DGTYAMJGM, las Leyes N° 14.828, 14.989, los Decretos N° 1018/16 y 34/18, la Resolución N° 251/15 de la Secretaría General de la Gobernación, y

CONSIDERANDO:

Que a fin de alcanzar una gestión pública de calidad que posibilite la provisión eficaz y eficiente de bienes y servicios públicos a los ciudadanos de la provincia de Buenos Aires de manera equitativa, transparente y efectiva, para una mayor integración y desarrollo de la sociedad, la Ley N° 14.828 creó el “Plan Estratégico de Modernización de la Administración Pública de la Provincia de Buenos Aires”;

Que el mencionado Plan se compone de un conjunto de programas, normas y procedimientos destinados a instalar en el ámbito provincial, un nuevo modelo de gestión pública de calidad que posibilite la provisión eficaz y eficiente de bienes y servicios públicos de manera equitativa, transparente y efectiva, mediante un proceso de reforma de los sistemas administrativos;

Que dentro de sus componentes se encuentran, entre otros, el “Sistema de gestión por resultados: Elaboración e implementación de Planes Estratégicos” y el “Gobierno electrónico y nuevas tecnologías de la información y comunicación” (art. 4°, Anexo único, la Ley N° 14.828);

Que de acuerdo a aquel cuerpo legal, el sistema de gestión orientado a resultados en la Administración Pública se implementa a través de diversos instrumentos, dentro de los cuales encuentra el objetivo fundamental de garantizar la seguridad de la información en toda la Administración Pública Provincial a través de la coordinación de respuestas ante los intentos de ataque o penetración a las redes informáticas de los organismos, fijando los estándares de seguridad y controlando que sean cumplidos en los sistemas de la propia Administración Pública (art. 5.5, Anexo único, Ley cit.);

Que, por su parte, el Gobierno Electrónico se realiza a través de variados instrumentos, entre los cuales se encuentra la “Seguridad Informática”, mediante la cual se procura aumentar los niveles de seguridad informática a partir de la construcción de la infraestructura necesaria para dar el tratamiento adecuado y proteger la información y los sistemas de la Provincia de Buenos

Aires con la intervención de las áreas con competencia en la materia (art. 9.4, Anexo único, Ley cit.);

Que a tales fines, la normativa vigente autoriza a la Autoridad de Aplicación o quien ésta designe, con intervención de la dependencia competente en la materia (I) a establecer los marcos normativos y operativos necesarios para aumentar el nivel de seguridad informática y (II) a fortalecer las capacidades de prevención, detección y atención de incidentes informáticos que pudieran afectar los sistemas críticos del Gobierno de la Provincia de Buenos Aires (art. 9.4, incisos 1 y 2 Anexo único, Ley cit.);

Que previo a la sanción de la Ley N° 14.828, la entonces Secretaría General de la Gobernación, dictó la Resolución N° 251 de fecha 10 de noviembre de 2015, a través de la cual se creó el EQUIPO PROVINCIAL DE RESPUESTAS A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, con el propósito de intervenir y proteger las infraestructuras estratégicas y críticas de la Administración Pública Centralizada, Descentralizada, Organismos de la Constitución y Entes Autárquicos (arts. 1 y 2, Res. cit);

Que el artículo 18, apartado 6 de la Ley de Ministerios, N° 14.989, encomienda al Ministerio de Jefatura de Gabinete de Ministros, entender en materia de modernización de la Administración Pública;

Que en ese orden, a través del Decreto N° 34/18 se aprobó la estructura orgánico - funcional del Ministerio de Jefatura de Gabinete de Ministros, asignando a la Subsecretaría para la Modernización del Estado las acciones de implementar el Plan Estratégico de Modernización de la Administración Pública de la Provincia de Buenos Aires, conforme los lineamientos establecidos en la Ley N° 14.828, Decreto reglamentario N° 1018/16 y normativa complementaria; diseñar, promover, establecer, impulsar y evaluar planes, programas, acciones, proyectos, y el/los sistema/s de gestión que tengan por objeto la modernización del Estado Provincial, así como, establecer lineamientos estratégicos y pautas de funcionamiento en los temas relacionados con la tecnología de información y telecomunicaciones;

Que en idéntico sentido, el aludido Decreto N° 34/18 le encomienda a la Dirección Provincial de Sistemas de Información y Tecnologías, el cometido de elaborar y proponer el Plan de Seguridad de la Información, alineado a estándares internacionales, para su aplicación en la Administración Pública Provincial;

Que, asimismo, es misión del Departamento de Seguridad Informática, dependiente de la mencionada Dirección Provincial, desarrollar e implementar un marco regulatorio y técnico en seguridad de la información para el Gobierno Digital y sociedad de la información y controlar su cumplimiento, como así también establecer mecanismos operativos, de control inherentes a los estándares de seguridad definidos para las áreas de informática y comunicaciones, entre otras atribuciones -Decreto N° 34/18-;

Que, en consideración de los avances tecnológicos, el ciberespacio es concebido como un escenario fundamental para el intercambio de datos e información, por lo cual resulta de vital importancia, adoptar medidas concretas para garantizar la seguridad del espacio virtual donde operan diferentes reparticiones del Estado Provincial;

Que, la utilización de comunicaciones virtuales implica la exposición a posibles ataques y amenazas a la seguridad de la infraestructura digital, que en caso de prosperar podrían generar graves incidencias en los sistemas, razón por la cual resulta de suma importancia y necesidad, contar con medidas especiales, que garanticen un adecuado funcionamiento de las infraestructuras;

Que, en pos de dar cumplimiento a las misiones y funciones que fueran asignadas por la normativa vigente a las áreas técnicas y con el fin de dar cumplimiento a los objetivos plasmados en el “Plan Estratégico de Modernización de la Administración Pública de la Provincia de Buenos Aires” (Ley N° 14.828), deviene imprescindible implementar acciones tendientes a prevenir las incidencias informáticas que pudieran suscitarse;

Que consecuentemente, corresponde reemplazar la Resolución N° 251/15 de la entonces competente Secretaría General de la Gobernación (Ley N° 13.757), a los fines de reforzar las prácticas de seguridad y de prevención respecto de la criticidad, así como, eventuales incidentes informáticos y/o de infraestructuras;

Que han tomado intervención la Dirección Provincial de Sistemas de Información y Tecnologías de la Subsecretaría para la Modernización del Estado y la Asesoría General de Gobierno;

Que la presente se dicta en virtud de las facultades conferidas por las Leyes N° 14.828 y 14.989 y los Decretos N° 1018/16 y 34/18;

Por ello,

**EL MINISTRO DE JEFATURA DE GABINETE DE MINISTROS
DE LA PROVINCIA DE BUENOS AIRES**

RESUELVE

ARTÍCULO 1º: Crear el EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES, identificado institucionalmente por las siglas CSIRT-PBA, el cual funcionará en el Departamento de Seguridad Informática de la Dirección Provincial de Sistemas de Información y Tecnologías dependiente de la Subsecretaría para la Modernización del Estado o la que en el futuro la reemplace.

ARTÍCULO 2º: Establecer que el EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA), intervendrá en la identificación y protección de las infraestructuras críticas y de los sistemas informáticos que den soporte a los activos de información críticos de la Administración Pública de la Provincia de Buenos Aires.

ARTÍCULO 3º: Instruir al EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA) a dictarse su propio reglamento, el cual será aprobado por la Dirección Provincial de Sistemas de Información y Tecnologías, o la que en el futuro la reemplace.

ARTÍCULO 4º: El EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA) estará integrado por el Director Provincial de Sistemas de Información y Tecnologías, quien oficiará de coordinador del equipo, y por los agentes que éste designe, entre aquellos que presten servicios en dicha dependencia, todos los cuales desempeñarán las acciones con carácter Ad-Honorem.

ARTÍCULO 5º: Conferir al EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA) las siguientes acciones:

- a) Coordinar y ordenar las acciones de los equipos de respuestas a incidentes de seguridad informática de las distintas dependencias de la Administración Pública de la Provincia de Buenos Aires y articular acciones con los demás equipos a nivel provincial, administrando toda la información sobre reportes de incidentes de seguridad y encausando sus posibles soluciones de forma organizada y unificada.
- b) Actuar como repositorio de toda la información sobre incidentes de seguridad informática, herramientas, técnicas de protección y defensa, estándares y buenas prácticas.
- c) Alertar sobre casos de detección de intentos de vulneración de activos informáticos críticos, así como de las vulnerabilidades encontradas en los mismos.
- d) Coordinar la prevención, tratamiento y respuesta a incidentes de seguridad informática dentro del ámbito de competencia, elaborando y promoviendo estrategias, prácticas y mecanismos necesarios para satisfacer las necesidades de seguridad.

- e) Actuar como enlace de comunicación en representación de la Provincia de Buenos Aires ante el equipo de respuesta para emergencias informáticas nacional CERT.
- f) Coordinar y realizar ejercicios de respuesta ante emergencias relacionadas con incidentes informáticos.
- g) Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Público Provincial.
- h) Elaborar planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas.
- i) Recomendar la incorporación de tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Provincial.
- j) Asesorar a los organismos sobre herramientas y técnicas de protección y defensa de sus sistemas de información.
- k) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten los organismos del Sector Público Provincial.
- l) Monitorear los servicios que el Sector Público Provincial brinda a través de la red de Internet y aquellos que se identifiquen como Infraestructura Crítica para la prevención de posibles fallas de Seguridad.
- m) Promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Provincial al público en general, como así también del rol compartido entre el Sector Público y Privado para el resguardo de la Infraestructura Crítica.

ARTÍCULO 6º: Establecer que el EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA) actuará en el marco de la Ley N° 25.326 de Protección de Datos Personales y su Decreto reglamentario N° 1558/01.

ARTÍCULO 7º: Establecer que las jurisdicciones y organismos determinados en el artículo 2º de la Ley N° 14.828 podrán, en tanto lo consideren necesario, designar un representante que funcionará como enlace entre el EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA DE LA PROVINCIA DE BUENOS AIRES (CSIRT-PBA) y la respectiva Jurisdicción u Organismo.

ARTÍCULO 8º: Derogar la Resolución N° 251/15 de la Secretaría General de la Gobernación.

ARTÍCULO 9º: Registrar, publicar, dar al Boletín Oficial, comunicar, pasar a la Dirección Provincial de Sistemas de Información y Tecnologías. Cumplido, archivar.